Copy to DD(CSA).
" " Sigs.6. W.O.

15 (I)

TOP SECRET "U".

PAGE 1.

TICOM/I-76.

Attached are POW interrogation reports on LEHWALD, HAUPTS, KLETT, and LAUERBACH, together with preliminary raw materials and interrogation report on Uffz. OSKAR WINGENDER.

All reports were received from HQ, Theatre Service Forces, European Theatre, Office of the Theatre Chief Signal Officer, Signal Intelligence Division under cover note dated 13 Aug. 1945.

TICOM

Copy No. 12..

30 Aug. 45

No. of pages 15

Distribution

British

1 Director
2 D.D.3
3 D.D.4
4 D.D. (N.S.)
5 D.D. (M.W.)
6 D.D. (A.S.)
7-8 A.D. (C.C.R) (2)
9 Lt.Col. Leathem

U.S.

26-27 OP 20-G (2) (via Lt Pendergrass)
28 G-2 (via Lt.Col. Hilles)
29-30 S.S.A. (2) (via Major Seaman)
31 Director, S.I.D. USFET (via Lt.Col. Johnson)

TICOM

10 Chairman
11-12 S.A.C. (2)
13 Cdr. Bacon
14 Cdr. McKenzie
15 Cdr. Tandy
16 Lt.Col. Johnson
17 Lt.Col. Lewis Powell
18 Lt. Cdr. Manson
19 Major Seaman
20 Major Morgan
21 Lt. Vance
22 Capt. Cowan
23 Lt. Fehl
24-25 Ticom Files (2)

Additional

32 S.A.C. for Signals 6 War Office

TOP SECRET "U".

PRISONER OF WAR INTERROGATION REPORT.

I. Interrogation of LEHWALD, HANS

II. Interrogation of HAUPTS, KARL HEINZ

III. Interrogation of KLETT, WERNER

IV. Interrogation of LAUERBACH, RAINER

IA, APPENDIX

IIIA, APPENDIX

Plus report of the Signal Intelligence service of the German Army written by Oberst Boetzel, General des Nachrichten Aufklaerungs

. . . . . .

I. Interrogation of HANS LEHWALD, Lieutenant, age - 25 years.

1. Personal History

a. Inducted September 1940, trained five months in Signal Intelligence in Horch Lehr Komp at Halle, From February 1941 February 1943 he was assigned to FNAST 2 (Feste Nachrichten Aufklaerungsstelle) at Muenster, where he worked as a radio operator.

b. In February 1943 he attended an Infantry Officers Training School where he received his commission in August.

c. In August he joined the newly activated Nachrichten Aufklaerungkomp 626, being stationed in the Ukraine, Lemberg and Roumania. At this time he became an evaluator (Auswerter). At the end of August 1944, he was appointed liaison officer from the company to the Eighth German Army. P/W was in the hospital for three months, and on his release was appointed liaison officer to Armeegruppe Oberrhein (under Himmler). This lasted until 13 January 1945 when the Armeegruppe dissolved. At this time he became liaison officer between Nacrichten Aufklaerung Abt 14 and the Nineteenth German Army, surrendering with them at Gebweiler.

2. Operational Experience

a. P/W Lehwald acted as liaison officer between Nachrichten Aufklaerung Abt 14 and the Nineteenth German Army. His work consisted in consolidating the daily reports received from Nachr. Fernaufkl. Komp. 626, Foste Nachr. Aufklaerungsstelle 3 and Nachr. Nahaufklaerungszug Mars, and presenting a daily Signal Intelligence report to Nineteenth Army G-2.

b. Details of operations of Nachr. Fernaufkl. Komp 626 have been included in another report (that of P/W Haupts). Feste Nachrichten Aufklaerungsstelle 3 consisted of a reception platoon of approximately 70 receivers and an evaluation platoon (Auswertezug) of between 25 and 30 men. This was broken down into a traffic analysis section, a breaking section, fusion (Inhaltsauswertung) section, D/F section, and a filing section containing diagrams of the nets, call signs, personalities, code names, and D/F results.

c. The deciphered messages together with the flyslips made out by the traffic analysts were given to the Intelligence Coordinators (Endauswerter). These men prepared the daily reports which went to G-2, to regiment and to nearby tactical units. A daily technical report (Netzmeldung) containing frequencies, call signs and procedural notes of all traffic intercepted was received by Lt. Lehwald as liaison officer.

d. Nachrichten Nahaufklaerungszug Mars, an element of Nachrichten Aufkl. Abt 14, was a unit of originally 50 men which had been reduced to approximately 18 men by the last few months of the war. It had 10 to 12 sets and 3 evaluators. Its. mission was to handle R/T traffic in general.

e. The P/W described the organization of the Armee Auswertestelle which was assigned to the Nineteenth German Army. It consisted of four Corps Evaluation Sections (Korps Auswertestelle or Kast) - KAST XIII A.K., KAST LXIV A.K., KAST XVIII SS A.K., and KAST LXXX A.K. These were small units of approximately 15-20 men. The P/W claimed all of them to be destroyed.

Observation

a. P/W was extremely nervous and on his guard at first. When attention was drawn to his hesitation, he stated he would give all information at his disposal if we would assure him it was not to be places at the disposal of the Russians and if he were further assured that the Americans were not planning to starve the Germans. His intelligence enabled him to realize the ridiculousness of his proposals when it was pointed out to him and he proceeded to give information without hesitation.

II. Interrogation of KARL HEINZ HAUPTS, Wachtmeister. Age: 26 years.

1. Personal History.

a. Entered Army 1 October 1938, 3rd Co. Sig. Bn. 26 in Kolnhorchfunker. Signal Bn 26 became later Long Range Intelligence Co. 620. (Monitored French, Belgian and Dutch Traffic).

b. Began intercepting English traffic in August 1939 when Company was sent to Atlantic Coast near Norderney Island. The Company moved later to area near Julich and Aachen to monitor Western European countries and later to the Eastern Front.

c. In December 1941 to March 1942, furlough to study chemistry in Koln.

d. In March 1942 to May, Führerhauptquartier for training in Russian traffic.

e. In May 1942 to Eastern Front where he was transferred to traffic evaluation in breaking section.

f. In January 1943 he became control chief (Endauswerter) and transferred to the newly organized 626th Long Range Sig. Intelligence Company. The Company was in training and was activated in January 1944 in Winniza (UKRAINE).

g. In October 1944 the Company was sent to Landau (PFALZ) where it was schooled in United States traffic and reorganized. They intercepted first the Third Army, later at times, the French First Army and the American Seventh Army. At last, on 1 May, they intercepted the First and Ninth American Armies.

h. His main field of occupation was organization, training of signal intelligence personnel in cipher procedures (RUSSIAN) or map coordinate systems (RUSSIAN and UNITED STATES).

2. Operational Experience

a. P/W Haupts was a Wachtmeister in the 626 Nachrichten Fernaufklaerungs Komp, a subordinate unit of Nachrichten Aufklaerungs Abt 14. The strength of the company was originally between 250 and 300 men, although it was considerably under strength when on the Western Front. Its mission was originally the interception of traffic of the First French Army and Seventh American Army and later that of our First, Third and Ninth Armies. There were 80-100 intercept operators, 10-15 D/F operators, 10-15 breakers, 5-7 translators, 10 traffic analysts and 3 control chiefs. These latter acted as intelligence coordinators (Endauswerter). One of them was an officer Lt. Wolfrum, who, according to Haupts, was new and inexperienced and handled chiefly administrative matters. The work was done by the two other, both NCO's of which Haupts was one.

The following S.O.P. of the 626 Fernaufklaerungs Komp was obtained from information from bothe Haupts and Uffz Kletts (see following interrogation report for details on the P/W).

b. From the Intercept Section messages and logs were delivered to the Auswertungs (Evaluation) Section. The breakers received the messages while the Traffic Analysts received the logs together with an operators log sheet containing the following information, 1) time of intercept, 2) frequency, 3) C/S of addressee, 4) liaison sign, 5) C/S of sender, 6) number assigned for D/F section to take bearings, 7) radio procedure, 8) message number, and 9) operator's remarks. The Traffic Analysts made diagrams of the nets, in most cases identified the groups and coordinated the results received from D/F. Their reports, together with the deciphered messages were received by the Endauswerter (Intelligence Coordinators) who fused the information into a daily report. Copies of this report were sent to Nachr. Aufklaerungs Abt 14 as well as to Corps or army if in the vicinity.

c. Haupts stated that the only code used by the Seventh Army was AF code. Considerable depth of traffic, at least 30 messages, was needed for breaking. He claimed all the alphabets to have been reconstructed due to constant spelling of names of towns. However numbers and long phrases were difficult to reconstruct.

d. Slidex proved easy to break. Clear text constantly gave clues to related code text. Most commonly used Slidex cards was number 5, used by recon units. In most instances Slidex cards were captured, thereby avoiding the necessity of reconstructing by analysis. However, when cards were reconstructed by analysis, they were only successful in working out positions of stock phrases, and alphabet letters. Numbers were difficult except when map coordinates were transmitted. P/W stated alphabet letters were found in only one position on Slidex card, showing operators were careless in selection of speller groups.

e. P/W stated that 117 Recon Troop of VI Corps used a system similar to Slidex having a much larger card and using complete alphabets on both vertical and horizontal strips and which changed only every 30 days. This sytem differed from Slidex in that no clear text was used, and was termed by the enemy "Random Mixed Alphabet 2B Procedure.

f. All M 209 traffic (called AM 1 system by P/W) was transmitted immediately to higher headquarters for analysis. The only entry known to P/W was when the three messages were transmitted using same indicators. He did not know of any other successful methods of attack on this system.

g. In the Intercept Section, 40 receivers were operating from 0600 to 2300 hours and 3 receivers between 2300 and 0600 hours. Twenty of these receivers were used on search between 1500 and 5000 Kcs. Close coordination with D/F was evidenced by the fact that D/F operators were on duty at all timese in the set room. Upon picking up a net, information on frequency, C/S, and procedure was immediately given to D/F operator, so that a bearing could be made. Our nets were identified by traffic broken, operators characteristics and captured S.O.I's. Up to 15 December our C/S book had been almost completely reconstructed with the help of captured sequence charts.

3. Observations.

a. P/W was extremely cocoperative and expressed his willingness to give all information he possessed. He mentioned that he had not been able to become an officer because his mother was a Chilean and he had a Jewish Grandmother. He was highly intelligent and appeared to have a thorough knowledge not only of the workings of radio intelligence but also of its organization in the German Army.

III. Interrogation of WERNER KLETT, Unteroffizier, Age: 38 yrs.

1. Personal History

A. Inducted April 1940. Assigned to Horch Lehr Komp in Halle for training in Signal Intelligence.

b. On 29 August 1940 assigned to Feste Horchstelle Stuttgart, (later Strasbourg .. Arcachon).

c. On 12 May 1942 assigned to Leitstelle des Nachrichten.

d. On 21 January 1945, Aufklaerungs West in Berlin - in Sept 1944 this moved to Zossen.

e. On 22 January 1945, transferred to Nachrichten Fernaufklaerungs.

f. On 26 March 1945, Komp 626.

2. Operational Experience

a. P/W Klett had been an evaluator (Auswerter) with the Leitstelle des Nachrichten Aufklaerungs, Gen. Stab des Heeres, OKH May 1942 until the end of January 1945. He worked on consolidation of reports of information received from various Signal Intelligence units (Nachr. Aufkl. Kommandeure, Feste Horchstellungen, etc.(see appended diagram of Sig Int organization). This information was consolidated into a Nachrichten Aufklaerungs Lagemeldung (called by P/W "NALM") of which 35 copies were distributed to OKH, Himmler, the Gestapo, the Geheimdienst, the various Nachr. Aufkl. Kommandeure, and various other higher units - (a diagram of the form of this report is appended).

b. Klett claimed the operations of the German Sig. Int. service were considered highly successful. He stated that in 1942 they had been able to construct a very complete picture of our army organization from their intercept of our clear text in the U.S. file card indices of our officers down to Captain, their units, and location were kept. This information was given to General Stab, Fremde Heere West, which issued pocket manuals of American Army Organization. It was conceded by the General Staff that 95% of the information contained in these manuals was gained by Radio Intelligence. When the invasion began, a complete picture of our army , the numberof troops in the U.S, in England, Corps, Division, even Company numbers as well as special units (Rangers, Transport Service, etc) was claimed by the P/W to have been constructed. File cards were kept containing the name of the unit, location in U.S., Port of Embarkation, APO number and location in England, and the subordinated units.

After the invasion, he stated we moved our units so fast it became increasingly difficult for their operators to find them. Great reliance was placed on their D/F system.

c. P/W stated that since December 1944 a section was established at the Leitstelle devoted to all types of voice traffic- commercial radio, news brodcasts, etc. He knew very little about this as it was kept highly secret, but imagined that aside from Intelligence to be gained, it might have been made use of for German propaganda.

d. At the end of January 1945 an order was issued that all men fit for combat were to be moved forward from the Leitstelle. None of them, however, were to be placed in combat, and accordingly, Klett was transferred to Nachr, Fernaufkl. Komp 626. His duties here in the remaining two months of the war were in general non operational and had no information to offer on the activities of this unit.

3. Observations

a. P/W was highly intelligent. He made it clear that in his willingness to furnish us with all the information at his disposal he did not wish to be considered a traitor. He was offering it for the "The Mutual benefit of the U.S. amd Germany". He stated he realized we would have to keep a close watch on Russia even as Germany had on Italy. The implication of Russia as a common enemy has been noted in all the P/W's interrogated.

IV. Interrogation of RAINER LAUERBACH. Obergefreiter, Age: 20 yrs.

1. Personal History

a. Inducted 22 June 1943. Until March 1944 he served as a radio operator with Nachrichten Abt 3 in Potsdam, handling traffic between Luftwaffe Groups on borders of Berlin for A.A. defense.

b. In March 1944 he was transferred to Nachr. Aufkl. ersatz und Ausbildungs Abt 40 at Weinheim (near Heidel).

c. In August 1944 he was sent to Rumania to join the newly activated Nachr. Aufkl. Komp 626 as an operator and retreated with the unit to Hungary. November 1944 found the company at Wilfersdorf (near Vienna) preparing to move to the Western Front. Here he studied American Traffic.

d. On 12 November the company joined the Nachr. Aufkl. Komp 624 at Landau and the following month moved to Eberteinberg (near Baden Baden). In March 1945, when captured, the company was at Kaidersbach in the vicinity of Stuttgart.

2. Operational History

a. P/W identified himself as an intercept operator having worked on both Russian and American traffic. He stated the Russians were easier to identify than the Americans because of their use of the double call signs.

b. Our link sign or single call sign system was very successful and did not identify the station or net; this was done by the breaking of messages was well s D/F. P/W also stated that the use of low power by our stations caused a wavering tone and along with the characteristics of the operators, which they studied, it was easy to identify the net over a period of days.

c. P/W also stated that the continued use of "INT" in asking for readability reports helped tell the difference between American and British operators.

d. The Germans used close system of monitoring the American nets. Every operator was assigned 50 kilocycles for search. This way all stations and units were covered very thoroughly.

3. Observations

a. P/W had been a radio operator throughout his army career. He was familiar with our AF and Slidex systems but knew nothing of the breaking of them. His knowledge of German systems was confined to Maschinen-Schluessel and Div Handschluessel with which he had come into contact only as an operator.

The Signal Intelligence Service of the German Army.

(Translation of a statement written by Oberst Boetzel, General des Nachrichten Aufklaerungs)

1. The staffs and formations of the Signal Intelligence Service were formerly a part of the Signal Corps. Accordingly, complete responsibility rested in the hands of the Chief of the Army Signal Service (Chef HNW) - until recently, Gen. Praun.

2. Until December 1944, there existed under the command of this Chef HNW a control station (Leitstelle) for Signal Intelligence which handled all matters pertaining to Signal Intelligence. At the beginning of 1945, with the appointment of a staff officer as General of Signal Intelligence (GNA), the old organization was coverted under this new staff.

3. However, the GNA had no final authority over the Kommandeure of Signal Intelligence appointed by the high commands of the Army Groups, but acted rather as the advisory councillor who answered all general questions and gave directions in general. His major aim was to furnish a unified and coordinated existence to the numerous units of Signal Intelligence on the various fronts. In addition he was to furnish higher command units with a consolidated report of information furnished to him by the various Army Groups, such as the Intelligence from Signal Intelligence situation reports East or West.

4. The Kommandeure of Signal Intelligence at Army Groups, under the command of the Signal Chiefs of these commands, were, however, themselves immediate supervisors of the Signal Intelligence units of the subordinated armies. These units consisted each of one Fernaufkl. (Strategical R.I.) Komp and one Nahaufkl. (Tactical R.I.) Komp. At Corps ther existed a so called Auxiliary Evaluation Staff, and at the Divisions a close range Signal Intelligence unit.

Organization of German Signal Intelligence Service.

1. A staff officer was appointed as General of Signal Intelligence at the Control Station for Signal Intelligence (Leitstelle der Nachrichtenaufklaerung). Under him were 8 Kommandeure der Nachrichten-Aufklaerung. These were located with the various Army Groups. Numbers 1,2,3, and 8 were concerned with the Russian Front, 7 with Italy, 4 formerly with the Balkans but later changed to Oberbefehl West, 5 was the Southern part of the Western Front, and 6 took care of 21st Army Group. Each Kommandeur had an evaluation center (Nachrichten Aufklaerung Auswertestelle) and from one to three Signal Intelligence Bns. There were two or more R.I. Coys. and /or permanent R.I. centers (Feste Nachrichten Aufkl. Stellen).

These latter had existed in peace time, handling diplomatic traffic, etc., but had been converted to military traffic during the war. There were 12 strategical R.I. Companies (Nachrichten Fernaufklaerungs Komp) and 17 Tactical R.I. Companies (Nachrichten Nahaufkl. Komp). The P/W's interrogated, however, claimed that there were no longer any operational differences between these R.I. Companies.

(see attached diagrams)

APPENDIX I-A
/LEHWALD/

Organization of Signal Intelligence Units of Nineteenth German Army (Attached to Nineteenth Army)

Signal Intelligence Bn 14

C.O.: Hptm Bode
Evaluation Officer: Oblt Fischer

Permanent R.I. Center 3 (FNAST 3)

C.O.: Oblt Rabeler

Tactical R.I. Platoon Mars

C.O.: Lt. LOECHELT

(Assigned to Nineteenth Army)

Army Evaluation Center

Corps Evaluation Center XIII A.K. (KAST)

Leader: Wtm Timm.

Corps Evaluation Center LXIV A.K.
Corps Evaluation Center XVIII S.S. A.K. Leader: Uffz Spitzgoebel.
Corps Evaluation Center LXXX A.K.

Leader: Wtm Baldau(?)

APPENDIX IIIA
/KLETT/

Form of report "Nachrichtenaufklaerungslage Meldung" furnished daily by Control Station Signal Intelligence to Higher units.

Signal Intelligence Situation Report

General Staff of the Army

Chief of Signal Service.

Control Station of Signal Intelligence.

Signal Intelligence Situation Report 7/1.

Atlantic Front

Twenty -first British Army Group
First Canadian Army
Army Corps Divisions

1. Infantry Rgt 15 is attacking from East to West.

2. ? Division was transferred to (Place name).

3. Infantry Rgt 12 occupying front sector (Place name) to (Place name) or (Map coordinates)

4. Arty attack Eastern border Caen to Roadfork (coordinates)

Here followed a list of officers known to be engaged with these units and broken down between nationality of their units)

Southern Front

(Same as above).

Balkans.

(Same as above)

The report was concluded with an account of the latest information picked up from all sources. This consisted of such items:

1. War Dept Washington stated that a new school for paratroops is to be opened at Camp Blanding, Fla.

2. Food situation in America is growing steadily worse.

TOP SECRET "U". TICOM/I-76.

3 August 1945

PRISONER OF WAR INTERROGATION REPORT

Uffz. OSKAR WINGENDER

A. Extract from interrogation report Nr. 96, dated 17 May 1945, and published at Camp 93 (CI), Ninth U.S. Army.

B. Summary of material written by the subject, and originally attached as an annex to the above report.

C. Additional information obtained from prisoner by TICOM team at 6824 Detailed Interrogation Center, M.I.S., U.S. Army.

Interrogation Report on Uffz. OSKAR WINGENDER.

A. The following section of the report is taken from a Ninth Army Prisoner of War Report.

SUBJECT: WINGENDER, Oskar (Uffz)

1. Subject, a German national, was arrested on 12 April 1945 in Ilmenau, Germany, by the 90th CIC Det. He was suspected of being a German soldier in civilian clothes and declared he was a cryptanalytic expert in the OKH. Interrogation established that Subject was to be discharged on 31 March 1945, but that his dischargo papers had not yet been handed him.

BACKGROUND:

2. Subject was born on 22 March 1916 in Cologne-Nippes, Germany. He completed his studies in the Real-gymnasium and then took up engineering. Subject's political background is socialistic. His father was an active member of the Socialist Party (SPD) and Subject himself was active in the "Reichsbanner" and the Socialist Workers' Youth (SAJ). After Hitler's accession to power, Subject's father continually had to change residence in order to escape arrest during one year. Later he settled down and was disturbed no longer, although both father and son were declared "politically unreliable".

ARMY CAREER:

3. Subject was drafted into the Army in November 1938. At first he was assigned to a Pioneer unit, but was transferred in October 1942 to the Signal Interpreters Replacement and Training Bn. in Meissen Saxony. After one month's training he was assigned to the OKH in Berlin, to the"Inspektion des Nachrichtenwesens", where he was trained in the cryptanalysis of British and American cryptographic systems. Subject was then assigned to "Referat 13, England". In March 1943, he was transferred to the NAAST 5 in St. Germaine-en-Laye, France, also to Referat 13. (FPN 47666). In April of the same year he was assigned to FNAST 3, Euskirchen, Germany (FPN 02700). In the course of his activities in these units, Subject became familiar with several of the English and American systems.

DISCHARGE:

4. In December 1943, Subject was indefinitely furloughed for study purposes under a program called "Sonderaktion fuer die Bereitstellung von Ingenieuren fuer die Ruestungsindustrie". Subject continued his engineering studies in Cologne until 15 March 1945, when he

passed the State examination for an engineering diploma and was employed by the Ortlinghaus firm in Montabaur. On 31 March, Subject was summoned to Ilmenau to hand in his military papers and be discharged from the service. However he was not given his discharge papers and was told to return after Easter. Subject, awaiting his final papers, remained in Ilmenau which was overrun by the American forces. He was arrested on 12 April.

B. The second section of the report is a summary of a statement written by the prisoner.

1. Cryptanalytic Organization in Wehrmacht.

a. Cryptanalytic sections existed in every branch of the Wehrmacht: Army, Navy, Airforce, Waffen S.S. and OKW. Cryptanalysts were trained in the headquarters of each branch. The prisoner's opinion was that Army cryptanalysts had greater success in their work than did cryptanalysts of other branches. The only text used in training was: Fletcher-Pratt, "QuelquesInquisitions sur la Cryptographie Moderne"

b. The prisoner knew of the following organisations in the Army:

(1) A Central Cryptanalytic-Headquarters in VII/6 (Inspektion der Nachrichtentruppen) in Berlin at Matteikirchplatz and Tirpitzufer. Here he worked in Referat 13, England under Inspektor Fischer.

(2) Subdiv. West.

(a) The chief officer was Komm. Gen. of the "Nachrichtentruppen West".

(b) The main unit was NAASt 5, Feldpost 47666 (Nachr. Aufklaerungs Auswerte Stelle), under the command of Major Deloliva (also written De Loeliva and Del Oliva), which was located in 1943 at Saint Germain-en-Laye, Paris, and in the Autumn, 1944, at Montabaur/ Westerwald. The prisoner worked in Referat 13, England, under Inspektor Liedtke.

(c) A subordinate unit of the above was FNASt 3 (Feste Nachr. Aufklaerungs Stelle) which was located in 1943 at Euskirchen/ Rheinland and in the autumn 1944 in the Schwarzwald. The heads of the cryptanalytic section of this unit were Oberwachtm. Glatzel and Uffz. Fischer.

2. Processing of Traffic.

a. The intercept units (NASt. - Nachrichten Aufklaerungs Stellen) were usually independent units, located according to intercept possibilities and subdivided according to the nets they covered.

b. From these units traffic was sent to:

(1) The NAASt above them.
(2) The central cryptanalytic headquarters in Berlin.

c. At the NAASt. traffic was registered and sorted by the "Auswertung". Messages in the clear and deciphered messages were translated into German.

d. Enciphered messages were given to the "EZ" squad by which a first sorting was made into four categories: hand enciphered systems, known machine systems, unknown machine systems, and unknown systems. The traffic of all machine systems was sent to Berlin.

e. The chief of the cryptanalytic section then distributed the traffic to the cryptanalysts, who were divided into teams of 2-6 men. Each team worked only on one type of system.

3. Cryptanalysis.

a. The cipher systems were first studied to determine whether they were substitution or transposition systems.

b. Transposition systems.

A system was first studied to determine if it was similar to a known system. Messages of the same length with the same key were then sought. When found, these were superimposed, anagrammed, and the transposition key recovered.

c. Substitution systems.

(1) Each system was studied statistically to determine whether it was mono- or polyalphabetic. Solution was achieved by a study of repetitions and the use of probable words.

(2) Probable words or stereotyped phrases were employed repeatedly by some nets. They often made possible the quick solution of new keys. The following phrase was found frequently by the prisoner.

DAILY FREIGHT / SHIPPING REPORT STOP IN (name of ship or harbor),

or NIL OUT (name of ship or harbor, or NIL signature. Other useful probable words were:

AVAILABLE, SICKCALL, URGENTLY REQUESTED, POINT, AIR-BASE, NO REPEAT NO.

4. Remarks on Allied Security.

The wireless service of England and, even more so, of U.S. forces often showed serious violations of radio discipline and cryptographic security. Congratulations on the occasion of an anniversary, etc., often revealed the structure of nets. Some nets were so well known that a change of call signs in a divisional net could be cleared up within six hours. Even fictitious stations and traffic were recognised.

Newspapers often revealed the names of units and officers, thereby providing probable words. Occasionally when a system was unknown by an Allied receiving station, the same message would be re-sent in another system without paraphrasing the text. In some cases German stations pretended to be an Allied receiving station and requested that a message, sent in an unknown system, be re-sent in a system which German cryptanalysts had already solved.

5. Other systems of which the prisoner had knowledge.

a. The prisoner was told by members of NAASt 5 during the autumn of 1944, that most movements of units of the invasion Army could be followed by deciphered messages. Hand-enciphered systems could usually be solved. He also knew of a small cipher machine of Swedish origin, bought by the English, which was in the possession of the OKW. All messages from the Italian theatre, enciphered by use of this machine, were read in Berlin.

b. 24 x 26 "Column-Caesar"

Once the 24 alphabets were known, solution proceded by the use of an IBM card index and probable words. 80% of all messages were deciphered within from six hours to two weeks. The system was employed in Iceland nets (Pheydar) of the Navy and in the States by the Air Force.

c. Tiger-code.

The code consisted of 3 letters, the middle of which was one of the vowels - A, E, I, O, U, Y. It was employed for the first time, during the big allied Tiger exercise in England and was solved in half a year in Berlin. The depth from which it was solved consisted of about 180 good messages. The entry into the code was made possible by means of a long report in an English paper containing names of officers and units. The spellers (?) of the code were found by the names of places and towns mentioned in the report. Similar codes were partly deciphered with less material within 2-3 months.
The correctness of the reconstructed code was verified, when, on the occasion of the Dieppe assault, a copy was captured.

C. The last section of the report, comes from further interrogation made by TICOM team at REVIN.

On further interrogation the Subject had, at best, vague recollection of details on matters discussed, particularly in respect to names and dates. Consequently, it is felt that many of the facts cannot be considered reliable. On many questions where the subject was indefinite or uncertain it was decided not to pursue the details involved. The only guidance that can be offered is to keep in mind the chronology of his activities at (1) Berlin (2) St. Germain and (3) Euskirchen.

1. 24 x 26 "Column-Caesar"

This system mentioned in his write-up, was probably U.S. M-94 or one of the earlier strip systems. The method of solution has been previously explained in the interrogation report on SCHWARTZE. However, Subject brought out the following points:

a. Text was sent in 5-figure groups.
b. He was not certain whether there were 24, 25, or 26 total strips, or letters on each strip, although he did mention 625 cards being used.
c. Settings changed daily at first and later every 6 or 8 hours.
d. The method for setting the order of the strips was not discovered.
e. The system was in use in 1943.
f. Berlin was reputed to have discovered the means by which the alphabets had been systematically constructed.
g. The card system used was five times quicker than previous methods.
h. Each card has between 12 and 15 punches.
i. A refinement for testing a probable word was developed later which used 25 films similar to the cards. The films containing the letters comprising the assumed word were selected and placed in a device which permitted rapid testing of possible strips by sliding the films into different positions. This method was about 10 times faster than the one previously employed.

2. Tiger Code:

The only addition of interest on this code was the fact that easily recognizable groups meaning "word follows of n groups (letters?)" were used and immediately followed by speller groups which were both single letter and syllabic in character. Repeated officers signatures were a great help in this respect.

3. English Code:

Prisoner worked on an English code of which he could not remember the name:

a. Germany has the basic book. He understood that England knew of the compromise.
b. Encode was on one side of the page and decode on the other.
c. It was mainly used for training in 1942 and 1943.
d. The code was enciphered by an additive.
e. The indicator was the second group of the message.
f. The indicator system was never solved.
g. Messages were solved by use of a difference catalogue. When asked to explain solution, he stated that messages were set by taking differences between all adjacent groups in the SAME message and looking for corresponding differences in other messages. When questioned more closely on this he insisted that the procedure has been as described but did not know why; he did admit however, that the catalogue did not list differences of this type.
h. Stretches of the additive were written around the walls of the room. The book had not been appreciably reconstructed.
i. Not too large a percentage of the traffic was read.
j. Either the additive or book was changed since it was not broken after 1943. He understood that Insp. Liedtke claimed to have a method for solution of the new version.

4. British Army Stencil

a. It was . fully solved including the indicator which took about one hour.
b. There were 25 columns of which 10 were not used.
c. The entire stencil was worked out on 80-100 messages.
d. The system later disappeared.

5. U.S. Division Field Code:

a. He remembers DFC 17, 19 and 21. They were most successful with the first two.
b. To his knowledge none were captured.
c. Only the 4-letter traffic was studied. All figure traffic was suspected of being machine and sent to Berlin.
d. The greatest weakness of the DFC was that the vocabulary remained constant.

6. Grid Systems:

Some work was done on grid systems at NA 5.

7. SSF:

SSF, of which he does not know the meaning, was, he believed, the designation of the radio-teletype intercept described below.

a. The American special receivers had a 6 or 8 impulse system.
b. Material was sent at hand speed.
c. At first, intercept was by tape and then read.
d. Machines were finally constructed, working under same conditions, which printed the text.

e. Traffic was varied, being mainly plain language, press telegrams and some coded signals, mostly unimportant.

f. A secret device was apparently added in the autumn of 1943. It was thought to involve a substitution. An effort was made to build a new machine but he heard no further details of the result.

8. Practice Tables:

Practice tables used in British W/T could be recognised as such.

9. RASTER:

Many Germans believe that the Raster employed by them could be solved in one afternoon. He did not offer to demonstrate, but merely added that a simpler and more effective system would be to send the message backwards in plain language. His attitude was sincere.

10. German Cryptanalysis:

a. He does not feel that German cryptanalysis was sufficiently ambitious, since he is sure that much more could have been accomplished.

b. Subject wrote theoretical dissertation on possible methods of breaking machine keys. Insp. Harms, whom he approached with the idea, did not consider his technique practicable. His approach involved the testing of two and a half million possible settings with 2,000 machines and 2,000 women which, after six months, would have yielded solution of one machine-enciphered message.

c. He understood that all machine systems had been considered unapproachable with the exception of the one mentioned to him at St. Germain (probably M-209). He was certain that his friends would have told him if, after his departure from Berlin, they had tried anything along the lines he had suggested.